

Символьные алгоритмы и программы вычисления булевых базисов Грёбнера

М. В. Зинин

ООО «Андер Девелопмент»
119072, Москва

Семинар «Компьютерная алгебра»
факультета ВМК МГУ и ВЦ РАН,
11 апреля 2012, Москва

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Несколько слов о базисах Грёбнера

Основная решаемая задача: определить принадлежность многочлена к заданному идеалу.

Единый подход к задачам, выражаемым в виде системы

- алгебраических
- дифференциальных
- конечно-разностных

уравнений.

Несколько слов о базисах Грёбнера

Основная решаемая задача: определить принадлежность многочлена к заданному идеалу.

Единый подход к задачам, выражаемым в виде системы

- алгебраических
- дифференциальных
- конечно-разностных

уравнений.

Связь с булевыми функциями

Множество булевых функций $\{1, x + y, xy\}$ **полно**.

Любую булеву функцию можно представить в виде полинома Жегалкина (булева многочлена):

$$\sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} \cdot x_{i_1} \cdot \dots \cdot x_{i_s} + a,$$

где $a, a_{i_1 \dots i_s} \in F_2$.

Каждая булева функция представима булевым многочленом **единственным** образом. Булево кольцо — **кольцо главных идеалов**.

Связь с булевыми функциями

Множество булевых функций $\{1, x + y, xy\}$ **полно**.

Любую булеву функцию можно представить в виде полинома Жегалкина (булева многочлена):

$$\sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} \cdot x_{i_1} \cdot \dots \cdot x_{i_s} + a,$$

где $a, a_{i_1 \dots i_s} \in F_2$.

Каждая булева функция представима булевым многочленом **единственным** образом. Булево кольцо — **кольцо главных идеалов**.

Связь с булевыми функциями

Множество булевых функций $\{1, x + y, xy\}$ **полно**.

Любую булеву функцию можно представить в виде полинома Жегалкина (булева многочлена):

$$\sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} \cdot x_{i_1} \cdot \dots \cdot x_{i_s} + a,$$

где $a, a_{i_1 \dots i_s} \in F_2$.

Каждая булева функция представима булевым многочленом **единственным** образом. Булево кольцо — **кольцо главных идеалов**.

Применение булевых базисов Грёбнера

- Криптоанализ (HFE)
- Задачи булевой выполнимости (SAT)
- Моделирование квантовых вычислений
- Проверка моделей
-

Цели работы и практическая значимость

Цели:

- Исследование существующих алгоритмов построения базисов Грёбнера и их возможностей.
- Разработка специализированного алгоритма для вычисления булевых базисов Грёбнера.
- Реализация разработанного алгоритма и оптимизация на основе эмпирических данных.
- Разработка программных пакетов.

Практическая значимость:

- Утилиты BJB и BPB.
- Пакет BIBasis в составе системы REDUCE.
- Пакет BIBasis в составе системы Macaulay2.

Цели работы и практическая значимость

Цели:

- Исследование существующих алгоритмов построения базисов Грёбнера и их возможностей.
- Разработка специализированного алгоритма для вычисления булевых базисов Грёбнера.
- Реализация разработанного алгоритма и оптимизация на основе эмпирических данных.
- Разработка программных пакетов.

Практическая значимость:

- Утилиты BJB и BPB.
- Пакет VIBasis в составе системы REDUCE.
- Пакет VIBasis в составе системы Macaulay2.

Апробация работы

- Международная конференция по компьютерной алгебре и дифференциальным уравнениям. «On computation of Gröbner bases over F_2 », Финляндия, Турку, 2007 г.
- 11-ая конференция по компьютерной алгебре. «Involutive algorithm for computation of Gröbner bases over F_2 », Россия, Дубна, 2007 г.
- 4-ое международное совещание «Квантовая физика и информация». «An algorithmic approach to solving polynomial equations associated with quantum circuits», Россия, Дубна, 2007 г.
- 12-ая конференция по компьютерной алгебре. «Study of involutive criteria efficiency in computation of Boolean Gröbner bases», Россия, Дубна, 2008 г.
- Международной конференция «Математическое моделирование и вычислительная физика». «On computation of Boolean involutive bases», Россия, Дубна, 2009 г.
- Международной конференция «Полиномиальная компьютерная алгебра». «Boolean involutive bases and SAT solving», Россия, Санкт-Петербург, 2010 г.
- 14-ая конференция по компьютерной алгебре. «BIBasis package for computing Boolean involutive and Gröbner bases in REDUCE and Macaulay2 computer algebra systems», Россия, Дубна, 2011 г.

- Gerdt V. P., Zinin M. V. Gröbner bases over F_2 // Computer Algebra and Differential Equations. Vol. 67. 2007. Pp. 59–68.
- Гердт В. П., Зинин М. В. Инволютивный метод вычисления базисов Грёбнера над F_2 // Программирование. 2008. Т. 34, № 4. С. 191–203.
- Gerdt V. P., Zinin M. V. A Pommaret Division Algorithm for Computing Gröbner Bases in Boolean Rings // Proceedings of ISSAC 2008. ISSAC'08. 2008.
- Гердт В. П., Зинин М. В. О роли инволютивных критериев при вычислении булевых базисов Грёбнера // Программирование. 2009. Т. 35, № 2. С. 90–97.
- Gerdt V. P., Zinin M. V. An algorithmic approach to solving polynomial equations associated with quantum circuits // Physics of Particles and Nuclei Letters. 2009. Vol. 6, no. 7. Pp. 521–525.
- Gerdt V., Zinin M., Blinkov Y. On computation of Boolean involutive bases // Proceedings of International Conference Polynomial Computer Algebra. 2009. Pp. 17–24.
- Гердт В. П., Зинин М. В., Блинков Ю. А. О вычислении булевых инволютивных базисов // Программирование. 2010. Т. 36, № 2. С. 117–125.
- Зинин М. В. Пакет `ViBasis` для вычисления булевых инволютивных базисов и базисов Грёбнера в системах компьютерной алгебры `REDUCE` и `Macaulay2` // Программирование. 2012. Т. 38, № 2. С. 92–101.

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Основные обозначения

- $F_2 = \{0, 1\}$ — поле Галуа характеристики 2;
- $\mathbb{X} = \{x_1, \dots, x_n\}$ — множество независимых переменных;
- $\mathbb{F}_2[\mathbb{X}]$ — кольцо многочленов от переменных $\mathbb{X}$ над полем $\mathbb{F}_2$;
- $\mathbb{B}[\mathbb{X}]$ — кольцо булевых многочленов от переменных $\mathbb{X}$;
- $\langle F \rangle$ — идеал, порожденный конечным множеством многочленов F ;
- $\succ$ — мономиальное упорядочение, $x_1 \succ x_2 \succ \dots \succ x_n \succ 1$;
- $M(u, U)$, $NM(u, U)$ — множество мультипликативных и немultiпликативных переменных монома u из конечного множества мономов U ;
- $NF(f, F)$ — нормальная форма многочлена f по модулю конечного множества многочленов F ;
- $\mathcal{P}$ — деление Поммаре;

Особенности булева кольца

Булево кольцо есть коммутативное **фактор-кольцо** вида:

$$\mathbb{B}[\mathbb{X}] := \mathbb{F}_2[\mathbb{X}] / \langle x_1^2 + x_1, \dots, x_n^2 + x_n \rangle.$$

Умножение — **идемпотентно**:

$$\forall b \in \mathbb{B}[\mathbb{X}] : b^2 = b,$$

Сложение — **нильпотентно**:

$$\forall b \in \mathbb{B}[\mathbb{X}] : b + b = 0.$$

Особенности булева кольца

Булево кольцо есть коммутативное **фактор-кольцо** вида:

$$\mathbb{B}[\mathbb{X}] := \mathbb{F}_2[\mathbb{X}] / \langle x_1^2 + x_1, \dots, x_n^2 + x_n \rangle.$$

Умножение — **идемпотентно**:

$$\forall b \in \mathbb{B}[\mathbf{x}] : b^2 = b,$$

Сложение — **нильпотентно**:

$$\forall b \in \mathbb{B}[\mathbf{x}] : b + b = 0.$$

Особенности булева кольца

Булево кольцо — кольцо **главных идеалов**, но базис, состоящий из одного булева многочлена $\{p\}$, **не обязательно** является базисом Грёбнера:

$$x_1, x_2 \in \langle x_1 x_2 + x_1 + x_2 \rangle \subset \mathbb{B}[x_1, x_2].$$

Ни одно мономиальное упорядочение **не является допустимым** в булевом кольце:

$$x_1 \succ x_2 \xrightarrow{\cdot x_1} x_1 \cdot x_1 \succ x_1 \cdot x_2 \longrightarrow x_1 \prec x_1 \cdot x_2$$

Особенности булева кольца

Булево кольцо — кольцо **главных идеалов**, но базис, состоящий из одного булева многочлена $\{p\}$, **не обязательно** является базисом Грёбнера:

$$x_1, x_2 \in \langle x_1 x_2 + x_1 + x_2 \rangle \subset \mathbb{B}[x_1, x_2].$$

Ни одно мономиальное упорядочение **не является допустимым** в булевом кольце:

$$x_1 \succ x_2 \xrightarrow{\cdot x_1} x_1 \cdot x_1 \succ x_1 \cdot x_2 \longrightarrow x_1 \prec x_1 \cdot x_2$$

Булевы базисы Грёбнера и инволютивные базисы

- Мономиальные **упорядочения** — без изменений
- **Деление** булевых мономов:
 $a \mid b = m, \deg(m) = \min\{\deg(m_i) \mid m_i \cdot a = b\}$
- **Нормальная форма** булевых многочленов — с учетом деления булевых мономов

- Булев **базис Грёбнера** G :

$$\forall f \in \langle F \rangle \quad NF(f, G) = 0$$

- Булев **инволютивный базис** L :

$$\forall f \in \langle F \rangle, \quad NF_{\mathcal{L}}(f, L) = 0$$

Булевы базисы Грёбнера и инволютивные базисы

- Мономиальные **упорядочения** — без изменений
- **Деление** булевых мономов:
 $a \mid b = m, \deg(m) = \min\{\deg(m_i) \mid m_i \cdot a = b\}$
- **Нормальная форма** булевых многочленов — с учетом деления булевых мономов
- Булев **базис Грёбнера** G :

$$\forall f \in \langle F \rangle \quad NF(f, G) = 0$$

- Булев **инволютивный базис** L :

$$\forall f \in \langle F \rangle, \quad NF_{\mathcal{L}}(f, L) = 0$$

Булевы базисы Грёбнера и инволютивные базисы

- Мономиальные **упорядочения** — без изменений
- **Деление** булевых мономов:
 $a \mid b = m, \deg(m) = \min\{\deg(m_i) \mid m_i \cdot a = b\}$
- **Нормальная форма** булевых многочленов — с учетом деления булевых мономов

- Булев **базис Грёбнера** G :

$$\forall f \in \langle F \rangle \quad NF(f, G) = 0$$

- Булев **инволютивный базис** L :

$$\forall f \in \langle F \rangle, \quad NF_{\mathcal{L}}(f, L) = 0$$

Булевы базисы Грёбнера и инволютивные базисы

- Мономиальные **упорядочения** — без изменений
- **Деление** булевых мономов:
 $a \mid b = m, \deg(m) = \min\{\deg(m_i) \mid m_i \cdot a = b\}$
- **Нормальная форма** булевых многочленов — с учетом деления булевых мономов
- Булев **базис Грёбнера** G :

$$\forall f \in \langle F \rangle \quad NF(f, G) = 0$$

- Булев **инволютивный базис** L :

$$\forall f \in \langle F \rangle, \quad NF_{\mathcal{L}}(f, L) = 0$$

Булевы базисы Грёбнера и инволютивные базисы

- Мономиальные **упорядочения** — без изменений
- **Деление** булевых мономов:
 $a \mid b = m, \deg(m) = \min\{\deg(m_i) \mid m_i \cdot a = b\}$
- **Нормальная форма** булевых многочленов — с учетом деления булевых мономов
- Булев **базис Грёбнера** G :

$$\forall f \in \langle F \rangle \quad NF(f, G) = 0$$

- Булев **инволютивный базис** L :

$$\forall f \in \langle F \rangle, \quad NF_{\mathcal{L}}(f, L) = 0$$

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 **Алгоритмы вычисления булевых базисов**
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Существующие алгоритмы построения базисов Грёбнера

Алгоритм Бухбергера

- 1965 год
- Редукция всех S -многочленов
- 2 критерия

Инволютивный алгоритм

- 1998 год
- Редукция всех немультимпликативных продолжений
- 4 критерия

Оба **не применимы** в $\mathbb{B}[X]$:

- Упорядочения недопустимы
- Не каждый синглтон — базис Грёбнера

Существующие алгоритмы построения базисов Грёбнера

Алгоритм Бухбергера

- 1965 год
- Редукция всех S -многочленов
- 2 критерия

Инволютивный алгоритм

- 1998 год
- Редукция всех немультпликативных продолжений
- 4 критерия

Оба не применимы в $\mathbb{B}[X]$:

- Упорядочения недопустимы
- Не каждый синглтон — базис Грёбнера

Существующие алгоритмы построения базисов Грёбнера

Алгоритм Бухбергера

- 1965 год
- Редукция всех S -многочленов
- 2 критерия

Инволютивный алгоритм

- 1998 год
- Редукция всех немультимпликативных продолжений
- 4 критерия

Оба **не применимы** в $\mathbb{B}[X]$:

- Упорядочения недопустимы
- Не каждый синглтон — базис Грёбнера

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов**
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов**
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Универсальный способ построения булевых базисов

Т.к. $\mathbb{B}[\mathbb{X}]$ есть фактор-кольцо, то возможен гомоморфизм колец:

$$\phi : \mathbb{F}_2[\mathbb{X}] \rightarrow \mathbb{B}[\mathbb{X}]$$

- $\{f_1, \dots, f_m\} \subset \mathbb{B}[\mathbb{X}]$, $\Phi = \{x_1^2 + x_1, \dots, x_n^2 + x_n\}$
- $\{f'_1, \dots, f'_m, \Phi\} \subset \mathbb{F}_2[\mathbb{X}]$
- применить любой алгоритм
- $\{g'_1, \dots, g'_k, \Phi'\} \subset \mathbb{F}_2[\mathbb{X}]$
- $\{g'_1, \dots, g'_k\} \subset \mathbb{B}[\mathbb{X}]$ — искомый базис

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов**
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - **Инволютивный алгоритм на основе деления Поммаре**
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Деление Поммаре

Определение: Для монома $u = x_1^{d_1} \cdots x_{k-1}^{d_{k-1}} x_k^{d_k}$, где $d_k > 0$ переменные x_j , $j \geq k$ назовем **мультипликативными** по Поммаре, все остальные — **немумультипликативными**.

Для $u = 1$ все переменные являются мультипликативными.

Деление Поммаре — **глобально**.

Разделение переменных монома на мультипликативные и немумультипликативные по Поммаре и свойство делимости по Поммаре **сохраняются** гомоморфизмом $\phi : \mathbb{F}_2[X] \rightarrow \mathbb{B}[X]$.

Деление Поммаре

Определение: Для монома $u = x_1^{d_1} \cdots x_{k-1}^{d_{k-1}} x_k^{d_k}$, где $d_k > 0$ переменные x_j , $j \geq k$ назовем **мультипликативными** по Поммаре, все остальные — **немумультипликативными**.

Для $u = 1$ все переменные являются мультипликативными.

Деление Поммаре — **глобально**.

Разделение переменных монома на мультипликативные и немумультипликативные по Поммаре и свойство делимости по Поммаре **сохраняются** гомоморфизмом $\phi : \mathbb{F}_2[X] \rightarrow \mathbb{B}[X]$.

Инволютивный алгоритм на основе деления Поммаре

Алгоритм Pommaret Basis

Input: $F \subset \mathbb{B}[X] \setminus \{0\}$ – конечный набор многочленов,

$\succ$ – мономиальное упорядочение;

Output: P – $\mathcal{P}$ –базис идеала $\langle F \rangle$;

```
1: выбрать  $f \in F$  с наименьшим  $\text{lm}(f)$  относительно  $\succ$ 
2:  $P := \{f\}$ ;  $Q := F \setminus \{f\} \cup \{f \cdot x \mid x \in NM_{\mathcal{P}}(f)\}$ 
3: while  $Q \neq \emptyset$  do
4:   выбрать  $q \in Q$  с наименьшим  $\text{lm}(q)$  относительно  $\succ$ 
5:    $Q := Q \setminus \{q\}$ ;  $h := \text{HeadNormalForm}_{\mathcal{P}}(q, P)$ 
6:   if  $h \neq 0$  then
7:     for all  $\{p \in P \mid \text{lm}(h) \mid_{\mathcal{P}} \text{lm}(p)\}$  do
8:        $P := P \setminus \{p\}$ 
9:        $Q := Q \cup \{p\} \setminus \{p \cdot x \mid x \in NM_{\mathcal{P}}(p)\}$ 
10:    end for
11:     $P := P \cup \{h\}$ ;  $Q := Q \cup \{h \cdot x \mid x \in NM_{\mathcal{P}}(h)\}$ 
12:  end if
13: end while
14:  $P := \text{AutoreduceTails}_{\mathcal{P}}(P)$ 
15: return  $P$ 
```

Корректность, завершаемость, оценки

Доказано, что инволютивный алгоритм Помаре **корректен** и **завершается** за конечное число шагов, как в случае $\mathbb{F}_2[X]$, так и $\mathbb{B}[X]$.

Получены оценки:

- В кольце $\mathbb{F}_2[X]$: $|P| \leq 2^n - 1$
- В кольце $\mathbb{B}[X]$: $|G| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} = \mathcal{O}\left(\frac{2^n}{\sqrt{n}}\right)$

Корректность, завершаемость, оценки

Доказано, что инволютивный алгоритм Помаре **корректен** и **завершается** за конечное число шагов, как в случае $\mathbb{F}_2[X]$, так и $\mathbb{B}[X]$.

Получены оценки:

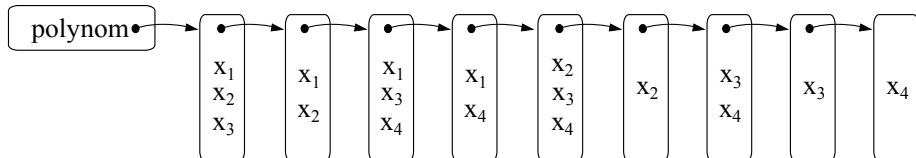
- В кольце $\mathbb{F}_2[X]$: $|P| \leq 2^n - 1$
- В кольце $\mathbb{B}[X]$: $|G| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} = \mathcal{O}\left(\frac{2^n}{\sqrt{n}}\right)$

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет `BIBasis` в системе `Macaulay2`
 - Пакет `BIBasis` в системе `REDUCE`
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами `Singular` и `PolyBoRi`
 - `Macaulay2`, сравнение `BIBasis` и `gb`
 - `REDUCE`, сравнение `BIBasis` и `Groebner`
- 6 Заключение

Представление булевых многочленов

$$x_1x_2x_3 + x_1x_2 + x_1x_3x_4 + x_1x_4 + x_2x_3x_4 + x_2 + x_3x_4 + x_3 + x_4$$



- Сложение 2-х многочленов: слияние сортированных списков.

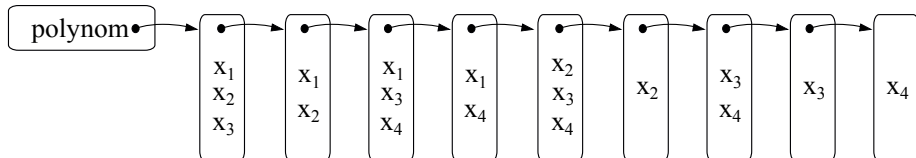
$$O(n * (l_1 + l_2))$$

- Умножение многочлена на переменную: разбить многочлен на 2 списка, умножить, слить списки.

$$O(n * l_1)$$

Представление булевых многочленов

$$x_1x_2x_3 + x_1x_2 + x_1x_3x_4 + x_1x_4 + x_2x_3x_4 + x_2 + x_3x_4 + x_3 + x_4$$



- Сложение 2-х многочленов: слияние сортированных списков.

$$O(n * (l_1 + l_2))$$

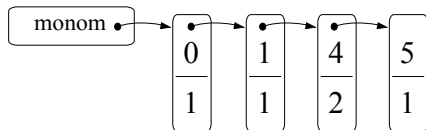
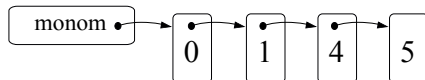
- Умножение многочлена на переменную: разбить многочлен на 2 списка, умножить, слить списки.

$$O(n * l_1)$$

Представление булевых мономов

[illegible]

Односвязный список:

$$x_0 x_1 x_4^2 x_5$$
 $x_0 x_1 x_4 x_5$ 

Выбор мономиального упорядочения

- Единственный класс мономов, отдельная функция-член класса для каждого упорядочения.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются фабрикой объектов, динамическое приведение.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются вызовами конструкторов. Все вышестоящие классы — шаблонные, параметр шаблона — мономиальное упорядочение.

Выбор мономиального упорядочения

- Единственный класс мономов, отдельная функция-член класса для каждого упорядочения.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются фабрикой объектов, динамическое приведение.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются вызовами конструкторов. Все вышестоящие классы — шаблонные, параметр шаблона — мономиальное упорядочение.

Выбор мономиального упорядочения

- Единственный класс мономов, отдельная функция-член класса для каждого упорядочения.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются фабрикой объектов, динамическое приведение.
- Базовый абстрактный класс мономов, класс-потомок для каждого упорядочения. Экземпляры классов создаются вызовами конструкторов. Все вышестоящие классы — шаблонные, параметр шаблона — мономиальное упорядочение.

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет **BIBasis** в системе Macaulay2
 - Пакет **BIBasis** в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение **BIBasis** и **gb**
 - REDUCE, сравнение **BIBasis** и Groebner
- 6 Заключение

Пакет BIBasis в системе Macaulay2

Язык реализации:

C++.

Представление данных:

разреженное, дистрибутивное, до 32767 переменных.

Выбор мономиального упорядочения:

шаблонные классы.

Пакет BIBasis в системе Macaulay2

Язык реализации:

C++.

Представление данных:

разреженное, дистрибутивное, до 32767 переменных.

Выбор мономиального упорядочения:

шаблонные классы.

Пакет BIBasis в системе Macaulay2

Язык реализации:

C++.

Представление данных:

разреженное, дистрибутивное, до 32767 переменных.

Выбор мономиального упорядочения:

шаблонные классы.

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет `BIBasis` в системе `Macaulay2`
 - Пакет `BIBasis` в системе `REDUCE`
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами `Singular` и `PolyBoRi`
 - `Macaulay2`, сравнение `BIBasis` и `gb`
 - `REDUCE`, сравнение `BIBasis` и `Groebner`
- 6 Заключение

Пакет BIBasis в системе REDUCE

Язык реализации:

Standard LISP.

Представление данных:

разреженное, дистрибутивное.

Выбор мономиального упорядочения:

специализированная функция для каждого упорядочения.

Пакет BIBasis в системе REDUCE

Язык реализации:

Standard LISP.

Представление данных:

разреженное, дистрибутивное.

Выбор мономиального упорядочения:

специализированная функция для каждого упорядочения.

Пакет BIBasis в системе REDUCE

Язык реализации:

Standard LISP.

Представление данных:

разреженное, дистрибутивное.

Выбор мономиального упорядочения:

специализированная функция для каждого упорядочения.

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Выбор тестовых примеров

Использованы серии:

- <http://www-sop.inria.fr/saga/POL/>
- life (Корняк'2005)
- <http://www.satlib.org/>

$$\begin{aligned}x \vee y &\longrightarrow xy + x + y \\ x \wedge y &\longrightarrow xy\end{aligned}$$

Машина:

- 2xXeon 5410 2.33Ghz
- 16Gb RAM
- Gentoo Linux
- gcc 4.4.3

Ограничения:

- 6 часов
- 10Gb RAM

Выбор тестовых примеров

Использованы серии:

- <http://www-sop.inria.fr/saga/POL/>
- life (Корняк'2005)
- <http://www.satlib.org/>

$$\begin{aligned}x \vee y &\longrightarrow xy + x + y \\ x \wedge y &\longrightarrow xy\end{aligned}$$

Машина:

- 2xXeon 5410 2.33Ghz
- 16Gb RAM
- Gentoo Linux
- gcc 4.4.3

Ограничения:

- 6 часов
- 10Gb RAM

Выбор тестовых примеров

Использованы серии:

- <http://www-sop.inria.fr/saga/POL/>
- life (Корняк'2005)
- <http://www.satlib.org/>

$$\begin{aligned}x \vee y &\longrightarrow xy + x + y \\ x \wedge y &\longrightarrow xy\end{aligned}$$

Машина:

- 2xXeon 5410 2.33Ghz
- 16Gb RAM
- Gentoo Linux
- gcc 4.4.3

Ограничения:

- 6 часов
- 10Gb RAM

Выбор тестовых примеров

Использованы серии:

- <http://www-sop.inria.fr/saga/POL/>
- life (Корняк'2005)
- <http://www.satlib.org/>

$$\begin{aligned}x \vee y &\longrightarrow xy + x + y \\ x \wedge y &\longrightarrow xy\end{aligned}$$

Машина:

- 2xXeon 5410 2.33Ghz
- 16Gb RAM
- Gentoo Linux
- gcc 4.4.3

Ограничения:

- 6 часов
- 10Gb RAM

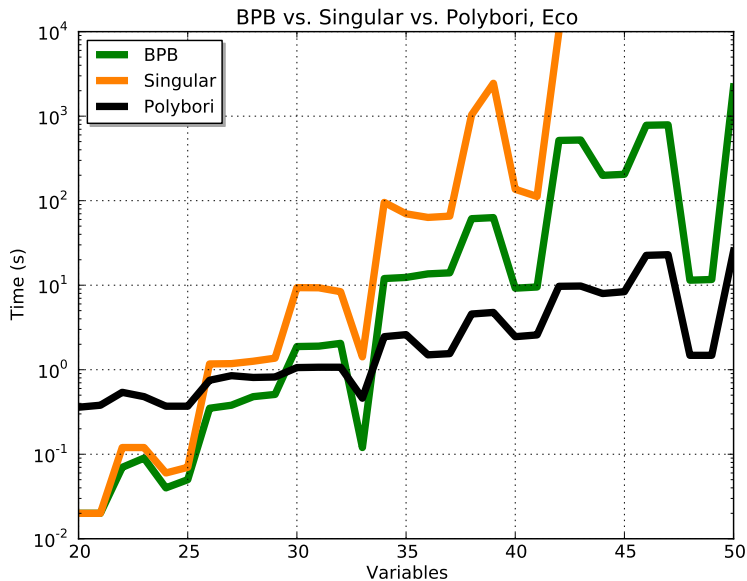
Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

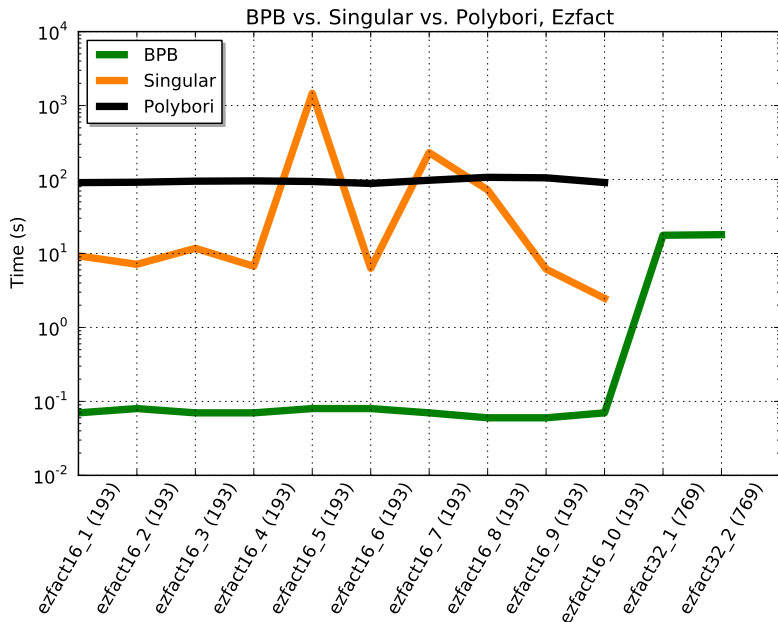
Сравнение с пакетами Singular и PolyBoRi

- PolyBoRi — открытый код, очень быстрая, специализирована для построения булевых базисов Грёбнера.
- Singular — открытый код, быстрая, система компьютерной алгебры общего назначения.

Сравнение с пакетами Singular и PolyBoRi



Сравнение с пакетами Singular и PolyBoRi



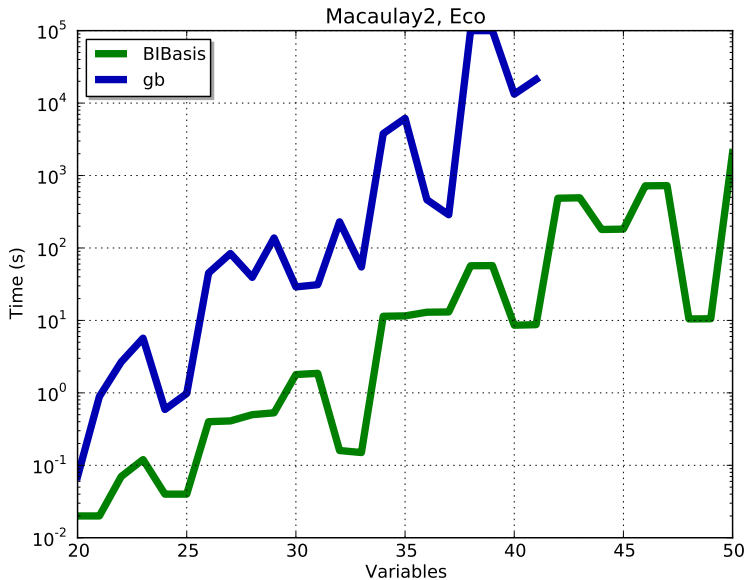
Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

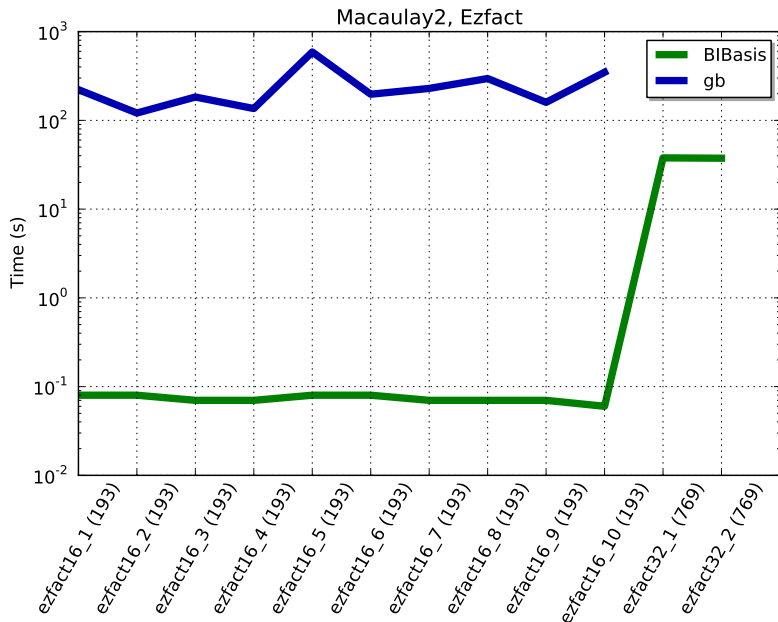
Macaulay2, сравнение BIBasis и gb

- Стандартный алгоритм gb — не специализирован для булевых вычислений, необходимо добавлять полевые биномы.

Macaulay2, сравнение BIBasis и gb



Macaulay2, сравнение BIBasis и gb



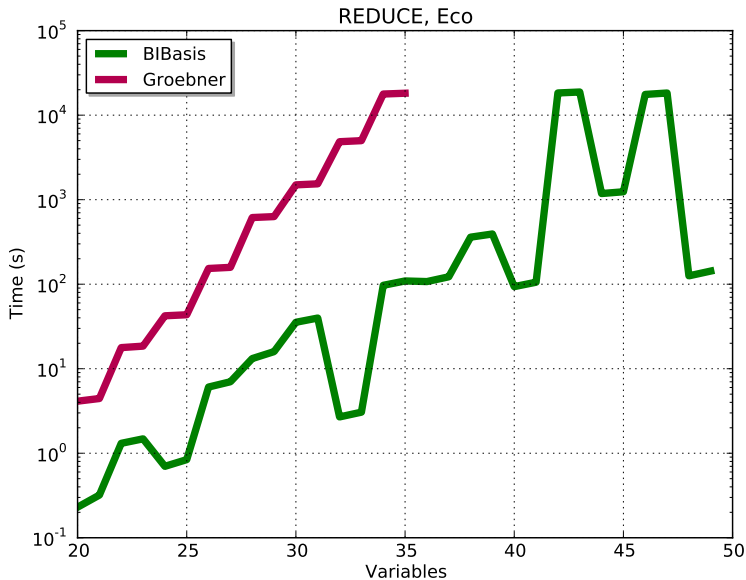
Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

REDUCE, сравнение BIBasis и Groebner

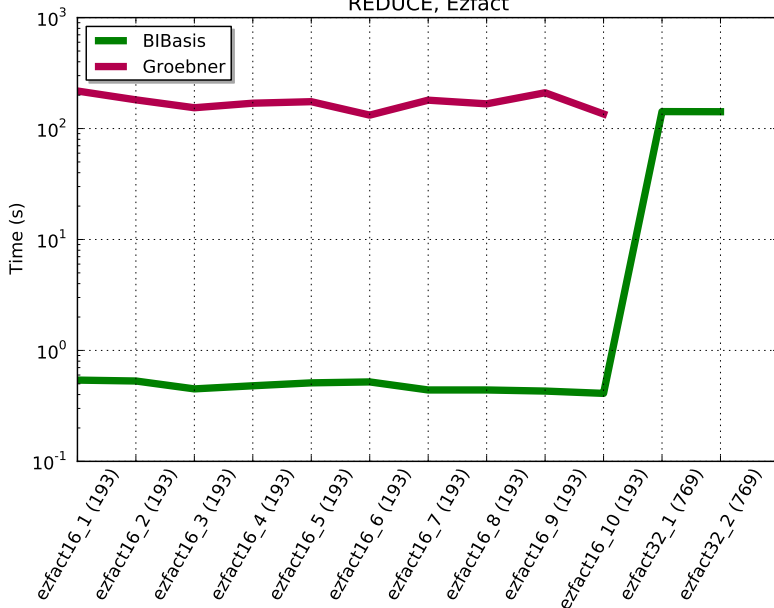
- Стандартный пакет Groebner — не специализирован для булевых вычислений, необходимо добавлять полевые биномы.

REDUCE, сравнение BiBasis и Groebner



REDUCE, сравнение BIBasis и Groebner

REDUCE, Ezfact



Выводы

- BPB быстрее BJB.
- BPB медленнее PolyBoRi, но быстрее Singular.
- BIBasis быстрее gb и Groebner.
- Производительность процессора важнее объема оперативной памяти.

Выводы

- BPB быстрее BJB.
- BPB медленнее PolyBoRi, но быстрее Singular.
- BIBasis быстрее gb и Groebner.
- Производительность процессора важнее объема оперативной памяти.

Выводы

- BPB быстрее BJB.
- BPB медленнее PolyBoRi, но быстрее Singular.
- BIBasis быстрее gb и Groebner.
- Производительность процессора важнее объема оперативной памяти.

Выводы

- BPB быстрее BJB.
- BPB медленнее PolyBoRi, но быстрее Singular.
- BIBasis быстрее gb и Groebner.
- Производительность процессора важнее объема оперативной памяти.

Содержание

- 1 Введение
- 2 Булевы базисы Грёбнера и инволютивные базисы
- 3 Алгоритмы вычисления булевых базисов
 - Существующие алгоритмы построения базисов Грёбнера
 - Универсальный способ построения булевых базисов
 - Инволютивный алгоритм на основе деления Поммаре
- 4 Программная реализация
 - Пакет BIBasis в системе Macaulay2
 - Пакет BIBasis в системе REDUCE
- 5 Результаты компьютерных экспериментов
 - Сравнение с пакетами Singular и PolyBoRi
 - Macaulay2, сравнение BIBasis и gb
 - REDUCE, сравнение BIBasis и Groebner
- 6 Заключение

Результаты

- Проведено **исследование применимости** инволютивного алгоритма к задаче построения базисов Грёбнера и базисов Жане в булевом кольце. Показано, что инволютивный алгоритм на основе деления Жане, как и алгоритм Бухбергера, может быть использован, но требует дополнения исходного булева базиса множеством всех полевых биномов. После этого вычисление базиса Грёбнера производится в кольце $\mathbb{F}_2[X]$, а искомый булев базис является подмножеством найденного базиса Грёбнера.
- Предложено **использование** инволютивного алгоритма на основе **деления Поммаре** для построения редуцированных булевых базисов Грёбнера и базисов Поммаре непосредственно в булевом кольце, т.е. без использования полевых мономов. Доказаны корректность и завершаемость указанного алгоритма. Показано, что он позволяет эффективно использовать представление булевых многочленов в памяти ЭВМ и простоту их арифметики.

Результаты

- Проведено **исследование применимости** инволютивного алгоритма к задаче построения базисов Грёбнера и базисов Жане в булевом кольце. Показано, что инволютивный алгоритм на основе деления Жане, как и алгоритм Бухбергера, может быть использован, но требует дополнения исходного булева базиса множеством всех полевых биномов. После этого вычисление базиса Грёбнера производится в кольце $\mathbb{F}_2[X]$, а искомый булев базис является подмножеством найденного базиса Грёбнера.
- Предложено **использование** инволютивного алгоритма на основе **деления Поммаре** для построения редуцированных булевых базисов Грёбнера и базисов Поммаре непосредственно в булевом кольце, т.е. без использования полевых мономов. Доказаны корректность и завершаемость указанного алгоритма. Показано, что он позволяет эффективно использовать представление булевых многочленов в памяти ЭВМ и простоту их арифметики.

Результаты

- Разработанный **булев инволютивный алгоритм** на основе деления Поммаре, а также алгоритм на основе деления Жане **реализованы** на языке программирования **Си++** в виде отдельных утилит. Дальнейшее изучение и сравнение быстродействия этих утилит между собой и с другими программными пакетами позволили отказаться от некоторых шагов алгоритма и найти компромисс между производительностью и функциональностью.
- На основе булева инволютивного алгоритма Поммаре создан **программный пакет** `ViBasis`, позволяющий строить редуцированные булевы базисы Грёбнера и Поммаре. Пакет **включен в состав** систем компьютерной алгебры `Macaulay2` и `REDUCE` с открытым исходным кодом и доступен под лицензией `GPL v2`.

Результаты

- Разработанный **булев инволютивный алгоритм** на основе деления Поммаре, а также алгоритм на основе деления Жане **реализованы** на языке программирования **Си++** в виде отдельных утилит. Дальнейшее изучение и сравнение быстродействия этих утилит между собой и с другими программными пакетами позволили отказаться от некоторых шагов алгоритма и найти компромисс между производительностью и функциональностью.
- На основе булева инволютивного алгоритма Поммаре создан **программный пакет** BIBasis, позволяющий строить редуцированные булевы базисы Грёбнера и Поммаре. Пакет **включен в состав** систем компьютерной алгебры Macaulay2 и REDUCE с открытым исходным кодом и доступен под лицензией GPL v2.

Ссылки

- **BJB** и **BPB**, исходные коды и версии для 64 разрядной ОС Windows:
<http://bpb.google.com>
- Пакет *BIBasis* в составе системы *Macaulay2*:
<svn://svn.macaulay2.com/Macaulay2/trunk/M2/Macaulay2/kernel/bibasis/>
- Пакет *BIBasis* в составе системы *REDUCE*:
<https://reduce-algebra.svn.sourceforge.net/svnroot/reduce-algebra/trunk/packages/bibasis/>